Editorial
Volume 13:2, 2022

Journal of Biometrics & Biostatistics

ISSN: 2155-6180 Open Access

Editorial Note on Biometrics and its Use

Yu Zhang*

Department of Statistics, Pennsylvania State University, Pennsylvania, USA

Editorial

Biometric is made up of two Greek words: Bio (life) and Metric (measurement) (to measure). Biometrics has been utilized for a variety of applications, including human identity and recognition based on physiological and behavioural features or attributes. Human physical traits such as appearance, body structures, and other factors are included. Various biometric traits such as 2D ridge-valley maps in fingerprints, face image, audio recordings of the voice, near-infrared images of the iris, video of gait motion, and others are extracted using computational techniques [1,2].

Are those that are linked to an individual's behavior (in certain aspects)? As a result, if a person's conduct differs from the stored behavioural pattern/profile, such biometrics verification can prevent them from authenticating/accessing. Voice, keystroke analysis, mouse dynamics, signature, and other biometrics are examples of this category. While biometrics applications are numerous, they are primarily divided into three categories: law enforcement, government, and commercial. Biometrics are increasingly being used in the commercial sector to secure authentication and confirmed transactions. ATM booths, credit cards, facility access, network login, online service, and data access are some examples of applications. Biometrics (both exterior and internal) are widely used in healthcare and medical science for blood transfusion, organ matching, identifying biological parents, ancestry, and other purposes.

Different biometrics are largely employed in two areas: real-world physical verification of humans and cyber-identity, authentication, and permission of legitimate access to computing systems and services. Identity verification in cyberspace is always difficult because it is difficult to determine who is on the other side of a virtual conversation in many cases. In particular, in both biometric and non-biometric authentication processes, it is impossible to validate legitimate user identification (from Spoofed) with 100% accuracy. Multi-factor authentication is becoming increasingly crucial for key Internet transactions and services to alleviate the problem. Similarly, physical biometric verifications have significant hurdles in the actual world for a variety of reasons, including: Due to the aforementioned considerations, as well as technological improvements in appearance and form shifting, it is becoming increasingly difficult to reliably identify humans based on physical characteristics, which can now be easily altered.

Furthermore, internal biometrics is emerging for human identity verification, if the aforementioned criteria are considered exterior biometrics. Internal features such as body pressure, blood type, and pulse rate are currently being used by forensic science to identify people, presuming that they are inert and difficult to modify, even though they need intrusive tests and can vary under stress and illness. In addition, organ transplantation, blood transfusion, immunotherapy, and hormone therapy may affect the body's internal biometrics; it was recently discovered that an astronaut's DNA changed by 7% after a year in space [3-5].

If the goal of using biometrics is to check human conduct (good, bad, harmful, harmless, authentic, non-genuine facts), the brain, which is irreplaceable and governs human behavior, should be the emphasis. As a result, human identity is mirrored in mental manifestations that may be seen in how a person acts in various circumstances and situations. We may be able to achieve a more accurate picture of a human's identification if we can precisely record the manifestation of brain activities or mind change (if it is the expression of brain function). A mind reader can deduce a person's true identity and behaviors from changes in the brain's electrochemical impulses. Researchers created a biometric brain print technology that can accurately identify people by detecting their EEG signals, which represent their brain processes. In general, each person's brain reacts differently to the same set of visuals. As a result, brain activity via EEG signals can identify every brain print (in other words, individuals) with pinpoint accuracy.

References

1. Snelick, Robert, Umut Uludag, Alan Mink, and Mike Indovina, et al. "Large scale evaluation of multimodal biometric authentication using state-of-the-art systems." *IEEE Trans Pattern Anal Mach Intell* 27 (2005): 450-455.
2. Jan, Farmanullah, Saleh Alrashed, and Nasro Min-Allah. "Iris segmentation for non-ideal Iris biometric systems." *Multimed Tools Appl* 7 (2021): 110.
3. Bullée, Jan-Willem H., Lorena Montoya, Wolter Pieters, and Marianne Junger, et al. "The persuasion and security awareness experiment: Reducing the success of social engineering attacks." *J Exp Criminol* 11 (2015): 97-115.
4. Jia, Lingyao, Xueyu Shi, Qiule Sun, and Xingqiang Tang, et al. "Second-order convolutional networks for iris recognition." *Appl Intell* 115 (2022): 1573-7497.
5. Sultana, Madeena, Padma Polash Paul, and Marina Gavrilova. "Social behavioral biometrics: An emerging trend." *Int J Pattern Recognit Artif Intell* 29 (2015): 1556013.

How to cite this article: Zhang, Yu. "Editorial Note on Biometrics and its Use." J Biom Biostat 13 (2022): 94.

***Address for Correspondence:** Yu Zhang, Department of Statistics, Pennsylvania State University, Pennsylvania, USA; E-mail: yzz2@psu.edu*

Received: 11 February, 2022, Manuscript No. jbmbs-22-64664; **Editor assigned:** 13 February, 2022, PreQC No. P-64664; **Reviewed:** 18 February, 202, QC No. Q-64664; **Revised:** 23 February, 2022, Manuscript No. R-64664; **Published:** 28 February, 2022, DOI: 10.37421/2155-6180.2022.13.94